ANDREW R. MUEHLBAUER, ESQ.
Nevada Bar No. 10161
MUEHLBAUER LAW OFFICE, LTD.
7915 West Sahara Avenue, Suite 104
Las Vegas, Nevada 89117
Telephone: 702.330.4505
Email: andrew@mlolegal.com

LOWEY DANNENBERG, P.C.
Christian Levis (*pro hac* vice forthcoming)
Henry Kusjanovic (*pro hac* vice forthcoming)
Amanda Fiorilla (*pro hac* vice forthcoming)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
clevis@lowey.com
hkusjanovic@lowey.com
afiorilla@lowey.com

LOWEY DANNENBERG, P.C.
Anthony M. Christina (*pro hac* vice forthcoming)
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA
Telephone: (215) 399-4770
achristina@lowey.com

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

KEVIN V. HORNE, on behalf of himself and all others similarly situated, Plaintiff, vs. MGM RESORTS INTERNATIONAL, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kevin V. Horne ("Plaintiff"), individually, by and through the undersigned counsel, brings this class action lawsuit against Defendant MGM Resorts International

("Defendant" or "MGM"), on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of counsel as follows:

INTRODUCTION

1. MGM is a publicly traded global entertainment and hospitality company that owns, operates, and manages hotels, casinos, and resorts, including the Mandalay Bay Resort and Casino located in Las Vegas, Nevada.

2. MGM publicly acknowledged on February 19, 2020, that in the summer of 2019, an individual gained unauthorized access to MGM's computer systems and downloaded Personally Identifiable Information ("PII") associated with more than 10.6 million guests. The PII stolen was highly sensitive and included names, addresses, driver's license numbers, passport numbers, military identification numbers, phone numbers, emails and dates of birth for guests who stayed at an MGM property through 2017.

3. This information was recently made available for download on the dark web, where it was posted to a hacking forum. Technology journalists at ZDNet and security researchers from Under the Breach were able to validate this data by using the disclosed PII to contact users and confirm that they stayed at an MGM property.

4. After being alerted of these findings, MGM separately confirmed that the data released on the dark web was that obtained during a July 2019 security incident.

5. Plaintiff was a guest at MGM's Mandalay Bay Resort and Casino during the period covered by the breach. In connection with this reservation, Plaintiff was required to provide MGM with PII, including his name, address, and driver's license number.

6. Plaintiff has been placed at an immediate and continuing risk of identity theft and other related harm as a direct result of MGM's failure to adequately protect his PII. Plaintiff, like

other Class members, will be required to undertake expensive and time-consuming efforts to mitigate the actual and potential impact of the data breach by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

7. Furthermore, Plaintiff and Class members will be required to purchase credit and identity monitoring services to alert them of potential misappropriation of their identities and to combat risk of further identity theft. At a minimum, Plaintiff and Class members have suffered compensable damages because they will be forced to incur the cost of a monitoring service which is a reasonable and necessary step to prevent and mitigate future loss.

THE PARTIES

8. Plaintiff Kevin V. Horne is a resident of the Commonwealth of Pennsylvania. In December 2017, Plaintiff stayed at the Mandalay Bay Resort and Casino in Las Vegas, Nevada, which is owned, operated, and managed by MGM.

9. In connection with this reservation, Plaintiff provided MGM with PII, including his name, address, and driver's license number.

10. Plaintiff first learned of the data breach on or about February 20, 2020.

11. Plaintiff has taken precautions to protect his PII. Exposure of Plaintiff's PII as a result of the data breach has placed him at immediate and continuing risk of further identity theft-related harm.

12. Defendant MGM is a publicly traded Delaware corporation with its principal place of business in Las Vegas, Nevada.

13. Defendant MGM is a global hospitality and entertainment company operating

hotels, casinos, and resorts throughout the world, including the Mandalay Bay Resort and Casino located in Las Vegas, Nevada.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 Class members, and at least one Class member is a citizen of a state different from the Defendant. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

15. This Court has general personal jurisdiction over MGM because it maintains its principal place of business in Nevada and therefore is at home in this District. The Court also has specific personal jurisdiction over MGM as it purposefully availed itself of the forum by engaging in suit-related conduct there, including the collection of PII from Plaintiff and Class members.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. MGM's Data Breach

17. On or about July 7, 2019, MGM recorded a data breach in which an individual or group of individuals gained unauthorized access to MGM's computer system and exfiltrated customer data. This data consisted of highly sensitive PII, including names, addresses, driver's license numbers, passport numbers, military identification numbers, phone numbers, emails and dates of birth of MGM customers.

18. The PII stolen in this data breach was subsequently posted on the dark web seven months later in February 2020. Technology journalists at ZDNet were the first to notify the public of this data dump, which contained PII for more than 10.6 million MGM guests that had stayed at an MGM property through 2017.[1]

19. ZDNet, in connection with security researchers from Under the Breach, were able to verify that this data was in fact from MGM by contacting guests whose PII was disclosed and confirming their stay at one of MGM's properties.

20. ZDNet promptly notified MGM of its findings. MGM then confirmed both that the data was from its systems and that it emanated from the July 2019 data breach.

21. According to Irina Nesterovsky, Head of Research at threat intelligence firm KELA, the data of MGM guests had been shared in some closed-circle hacking forums since at least July 2019. The hacker who released this information is believed to be associated with, or be a member of GnosticPlayers, a hacking group that has dumped more than one billion user records on the dark web.

22. While MGM did not publicly acknowledge that a data breach occurred until

---

[1] *See* Catalin Cimpanu, *Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum*, ZDNET, (Feb. 19, 2020), https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/.

February 2020, it appears that it began notifying certain customers of the breach in late 2019.[2] For example, at least some MGM customers received the Notice of Data Incident ("Notice") quoted in relevant part below in or around September 2019:

Notice of Data Incident

What Happened

On or about July 7, 2019, an individual accessed MGM Resorts International's computer network system without permission. The individual downloaded partial customer data from MGM's computer systems, then posted and disclosed part of the data on a closed internet forum. No customer financial information, passwords or credit cards were part of the data in question and it was taken down and removed from the closed internet site.

What Information Was Involved

MGM immediately initiated an internal forensic investigation into this incident. MGM conducted an exhaustive investigation and search of the downloaded data from the closed internet site. On August 9, 2019, MGM determined your First Name, Last Name, and Driver's License Number were part of the compromised file. Again, no financial information, passwords or credit cards were included in the database.

What We Are Doing

We take the security of our customers' data seriously, and after MGM became aware of the event, we took immediate measures to investigate and remediate the incident. We have implemented additional safeguards to improve further data security related to external software incidents. Furthermore, MGM reported the incident to law enforcement immediately once MGM discovered the matter. In addition, we are offering identity theft protection services through ID Experts®, the data incident and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

---

[2] *See Data breach at MGM Resorts in July 2019?*, VEGASMESSAGEBOARD, https://www.vegasmessageboard.com/forums/index.php?threads/data-breach-at-mgm-resorts-in-july-2019.165346/ (last visited Feb. 26, 2020).

> **What You Can Do**
>
> We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 833-959- 1344 or going to https://ide.myidcare.com/mgmri and using the Enrollment Code provided above.
>
> ***
>
> A gain, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

23. MGM's public acknowledgement of the data breach in February 2020 has only increased the risk to Plaintiff and the Class by drawing even more attention to the fact that their PII is available on the dark web.

B. MGM Privacy Policies

24. MGM maintains a Privacy Policy wherein it details the PII it collects from customers and promises to maintain the security and integrity of such data.

> **MGM RESORTS PRIVACY POLICY[3]**
>
> MGM Resorts International values your patronage and respects your privacy. This Privacy Policy ("**Policy**") describes the information collection, use, protection, and sharing practices of MGM Resorts International and MGM Resorts International web sites, mobile applications, electronic communications, and properties
>
> We collect information from a variety of sources and in a variety of ways, including the following:

---

[3] *See Privacy Policy*, MGM RESORTS INTERNATIONAL, https://www.mgmresorts.com/en/privacy-policy.html (last visited Feb. 26, 2020).

> **Personal Information.** When you visit, use, and/or access MGM Resorts or MGM Online Services, you may provide us with (and/or we may collect) information by which you can be personally identified including your name, date of birth, postal address, e-mail address, and telephone number, and videos, recordings, and images of you ("**Personal Information**"). We may also obtain Personal Information from third parties.
>
> **Sensitive Information.** When you make a purchase, visit, use and/or access MGM Resorts or MGM Online Services, or engage in other transactions or activities, you may provide us with sensitive Personal Information including your credit or debit card number, financial account number, biometrics, medical/health-related information, driver's license number, government-issued identification card number, social security number, passport number, or naturalization number ("**Sensitive Information**").
>
> **SECURITY**
>
> Information maintained in electronic form that is collected by MGM Resorts International and any individual MGM Resort is stored on systems protected by industry standard security measures. These security measures are intended to protect these systems from unauthorized access. No security system is impenetrable and these systems could become accessible in the event of a security breach. We have controls in place that are designed to detect potential data breaches, contain and minimize the loss of data, and conduct forensic investigations of a breach.
>
> Our staff is required to take reasonable measures to ensure that unauthorized persons cannot view or access your Personal Information. Employees who violate our internal privacy policies are subject to disciplinary action, up to and including termination of employment.

25. Although MGM claims to employ "industry standard security measures," this representation, along with the promise to maintain the integrity of customer PII is contradicted by its failure to impose and maintain the necessary safeguards that would have prevented the data breach.

C. The Data Breach Caused Harm to Plaintiff and Class Members

26. MGM failed to safeguard and protect its customers' highly sensitive PII including, but not limited to, customer names, addresses, driver's license numbers, passport numbers, military identification numbers, phone numbers, emails, and dates of birth.

27. The data leaked from MGM is a treasure trove of contact details and other PII. Plaintiff and Class members now face a higher risk of identity theft, receiving spear-phishing emails intended to gain further access to their own computer systems, and unwanted telemarketing phone calls, among other things. The adverse effects suffered by Plaintiff and the Class are compounded by MGM's failure to acknowledge the breach for seven months, depriving Plaintiffs and Class members of taking adequate precautions to protect their identify in advance of the February 2020 data dump.

28. MGM knew or should have known, based on the type and amount of PII it collected, that it was a target for hackers and should have implemented appropriate security measures designed to prevent a data breach. According to a 2018 report by information security company Trustwave, the hospitality sector is one of the top three industries most vulnerable to data breaches. Other industry publications estimate that hotels are targets in around 20 percent of all cyberattacks.[4] Indeed, in recent years, Marriott, Hilton, Hyatt, and Trump hotels have all faced data breaches. "Such unfortunate trends should not come as much of a surprise since hotels are hotbeds of sensitive information. Their data is spread out across porous digital systems and their sales are usually conducted through weak point-of-sale systems." *Id.*

29. "While hospitality companies have fewer transactions than retail organizations — and thus have data on fewer customers to steal — they collect substantially more valuable and varied personal data for each of their guests . . . This rich personal data is invaluable to

---

[4] Lena Combs, Joshua Davis, *Why cybersecurity matters*, HOTEL MANAGEMENT, (Oct. 17, 2019 10:40am), https://www.hotelmanagement.net/tech/why-cybersecurity-matters.

cybercriminals. They can use this data to better impersonate each breached customer, leading to additional identity theft and social engineering attacks against each individual's company. By enabling further attacks, breaching a hotel provides cybercriminals much more value than breaching a company in almost any other industry."[5]

30. PII such as customer names, addresses, driver's license numbers, passport numbers, military identification numbers, phone numbers, emails, and dates of birth—the same information exfiltrated in the MGM breach—is highly valuable to hackers as it can be used to steal a person's identify or commit a variety of financial crimes.

31. MGM's failure to implement and maintain reasonable security procedures and practices appropriate to protect Plaintiff's and Class members' PII also violated various federal and state cybersecurity guidelines. For example, the Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices, including PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS.[6]

32. Under the FTC guidelines, businesses should protect the personal customer

---

[5] Nirmal Kumar, *Cybersecurity in Hospitality: An Unsolvable Problem?*, PALADION, https://www.paladion.net/cybersecurity-in-hospitality-an-unsolvable-problem (last visited Feb. 26, 2020).

[6] FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

33. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 (2006). MGM's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

34. MGM, as one of the largest hospitality groups in the world, was fully aware of its obligation to protect customers' PII in accordance with state and federal law and industry guidelines. MGM was also aware of the significant consequences that Plaintiff and the Class would suffer if it failed to do so, as the harm caused by identify theft was widely discussed in the media, including industry publications warning hospitality groups that they were among hackers' favorite targets.

35. Despite understanding the consequences of maintaining inadequate security systems, MGM failed to adopt and maintain appropriate security measures to protect and secure customers' PII, including Plaintiff and Class members.

36. In the case of a data breach, merely reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[7]

37. A victim whose PII has been stolen and compromised may not see the full extent of identity theft or fraud until years after the initial breach. It may take some time for the victim to become aware of the theft. In addition, a victim may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

38. According to the BJS, an estimated 16.6 million people were victims of one or more incidents of identity theft in 2012.

39. MGM's failure to notify Plaintiff and the Class of the July 2019 data breach put them at a considerable disadvantage as they were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their PII for months without being able to take necessary precautions to prevent imminent harm.

40. As a result of the data breach, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are also subject to a higher risk of phishing where hackers exploit

---

[7] *See* Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, U.S. Dep't of Justice, Bureau of Justice Statistics (Dec. 2013), at 1.

information they have already obtained, *e.g.*, from the MGM data breach, to gain access to Plaintiff's and Class member's computer systems.

41. The exposure of Plaintiff's and Class members' PII to unauthorized individuals was a direct and proximate result of MGM's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure. MGM failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII in order to protect such PII against reasonably foreseeable threats to the security of such information.

42. Plaintiff's and Class members' PII is private and sensitive in nature and was inadequately protected by MGM.

43. As one of the nation's largest hotel and resort brands, MGM had the resources to implement security controls to prevent such a data breach. However, MGM has neglected to adequately invest in data security, despite the growing number of data intrusions and several years of well-publicized hospitality industry data breaches.

44. Had MGM remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted measures recommended by the FTC and experts in the field, MGM could have prevented hackers from gaining access to its computer systems and stealing Plaintiff's and Class members' confidential PII.

45. MGM's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure, compromising and theft of their PII;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized parties and misused via the publication of Plaintiff's and Class members' PII on the internet black market and dark web;

c. The untimely and inadequate notification of the data breach;

d. Loss of privacy;

e. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

f. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

g. Loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

h. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the data breach.

46. In response to the data breach, MGM has arranged with ID Experts® to provide "12 months of credit and CyberScan monitoring." This is inadequate. Plaintiff's and Class members' PII cannot be recovered once it its disclosed and therefore may exist on the dark web for months, or even years, before it is used by hackers. With only one year of monitoring, Plaintiff and Class members remain unprotected from the real and long-term threats against their PII. Plaintiff and Class members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

47. Plaintiff, Kevin V. Horne, brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all others similarly situated, as representative of the following Class:

> All persons residing in the United States who provided PII to Defendant and whose PII was accessed, compromised, or stolen as a result of the July 7, 2019 data breach.

48. The aforementioned Class is referred to herein as the "Class."

49. Excluded from the Class are affiliates, predecessors, successors, officers, directors, agents, servants, or employees of Defendant, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action and their law clerks, court personnel and their family members, and any juror assigned to this action.

50. Plaintiff reserves the right to amend the Class definition if discovery and/or further investigation reveal that it should be modified.

51. The members of the Class are so *numerous* that the joinder of all members of the Class in single action is impractical. MGM has acknowledged that approximately 10.6 million MGM hotel guests had their data exposed and for over seven months. The Class members are readily identifiable from information and records in Defendant's possession, custody, or control, including those reflecting reservations during the relevant period.

52. There are *common questions of law and fact* to the Class members, which *predominate* over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant owed a duty to Plaintiff and Class members to safeguard and protect the security of their PII;

b. Whether Defendant failed to use reasonable care and commercially reasonable methods

to secure and safeguard Plaintiff's and Class members' PII;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' PII from unauthorized capture, dissemination and misuse;

53. Plaintiff's claims are *typical* of those of other Class members because Plaintiff's PII, like that of every other Class member, was misused and improperly disclosed by Defendant.

54. Plaintiff will fairly and *adequately represent* and protect the interests of the Class. Plaintiff has retained competent counsel experienced in litigating complex class actions, including consumer class actions. Plaintiff intends to prosecute this action vigorously. Plaintiff's claims are typical of the claims of all of the other Class members, and Plaintiff has the same non-conflicting interests as the other Class members. Therefore, the interests of the Class members will be fairly and adequately represented by Plaintiff and his counsel.

55. A class action is *superior* to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go unremedied.

56. Class certification is appropriate under Federal Rules of Civil Procedure 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, such that final injunctive or corresponding declaratory relief is appropriate to the Class as a whole.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

(Negligence)

57. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

58. MGM owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

59. This duty included, among other things, designing, maintaining, and testing MGM's security systems to ensure that Plaintiff's and Class members' PII was adequately secured and protected. MGM further had a duty to implement processes that would detect a breach of their security system in a timely manner.

60. MGM also had a duty to timely disclose to Plaintiff and Class members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and Class members could take appropriate measures to protect their identity by, among other things, monitoring their accounts for unauthorized access, contacting the credit bureaus to "freeze" their accounts, place alerts, and take all other appropriate precautions.

61. MGM breached is duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information; allowing unauthorized access to Plaintiff's and Class members' PII stored by MGM.

62. MGM breached its duty to timely disclose that Plaintiff's and Class members' PII

had been, or was reasonably believed to have been, stolen or compromised.

63. MGM's failure to comply with industry regulations and the delay between the date of intrusion and the date MGM acknowledged the data breach further evidence MGM's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII.

64. But for MGM's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised, stolen, and viewed by unauthorized persons.

65. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of MGM's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII. MGM knew or should have known that their systems and technologies for processing and securing Plaintiff's and Class members' PII had security vulnerabilities susceptible to hacking.

66. As a result of MGM's negligence, Plaintiff and Class members incurred damages including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of MGM's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; and irrecoverable financial losses caused by identity thieves who wrongfully gained access to Plaintiff and Class members' PII.

SECOND CLAIM FOR RELIEF

(Negligence *Per Se*)

67. Plaintiff repeats, realleges, and incorporates by reference the allegations

contained in each and every paragraph above, as though fully stated herein.

68. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the failure to use reasonable measures to protect customer PII.

69. MGM violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class members' PII and by not complying with industry standards. MGM's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, public reports in industry publications that hospitality groups were being targeted by hackers, and the foreseeable consequences of a data breach at one of the nation's largest hotel and resort brands.

70. MGM's violation of Section 5 of the FTC Act constitutes negligence *per se*.

71. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

72. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

73. As a direct and proximate result of MGM's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

(Breach of Contract)

74. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

75. MGM expressly promised to safeguard Plaintiff's and Class member's PII. Specifically, MGM promised to abide by their privacy policy, which is made available to all MGM guests.[8]

76. This policy applied to Plaintiff and Class members, who entered into a contract with MGM when they provided their PII to MGM as part of a transaction in which they paid money in exchange for the right to stay at an MGM property.

77. Plaintiff and Class members fully performed their obligations under the contracts with MGM, including by compensating MGM for their stay at an MGM property.

78. MGM did not hold up their end of the bargain. In entering into such contracts, MGM agreed to protect Plaintiff and Class members PII in accordance with their privacy policy, including storing such information "on systems protected by industry standard security measures." Additionally, MGM ensured Plaintiff and Class members that it "ha[d] controls in place that are designed to detect potential data breaches, contain and minimize the loss of data, and conduct forensic investigations of a breach."

79. MGM failed on both accounts: MGM did not have industry standard security measures in place, nor did it have controls designed to detect, contain, and minimize the loss of data in the event of a data breach. Each of these acts constitute a separate breach of the contracts

---

[8] *See Privacy Policy*, MGM RESORTS INTERNATIONAL, https://www.mgmresorts.com/en/privacy-policy.html (last visited Feb. 26, 2020).

MGM entered with Plaintiff and Class members.

80. Plaintiff and Class members would not have entrusted MGM with their PII in the absence of the contract between them and MGM, obligating MGM to keep this information secure and take reasonable measures to ensure that unauthorized persons cannot access PII.

81. As a direct and proximate result of MGM's breaches of their contracts, Plaintiff and Class members did not receive the full benefit of their bargain and instead received services that were less valuable than what they paid for. Plaintiff and Class members were damaged in an amount at least equal to this overpayment.

FOURTH CLAIM FOR RELIEF

(For Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law)

P.S. § 201-1, *et seq.*)

82. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

83. As a consumer of MGM's services, Plaintiff is authorized to bring a private action under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). 73 P.S. § 201-9.2.

84. Plaintiff is a "person" within the meaning of 73 P.S. § 201-2(2) because he is a "natural person[]".

85. Plaintiff and Class members provided their PII to MGM pursuant to transactions in "trade" and "commerce" as meant by 73 P.S. §201-2(3), for personal, family, and/or household purposes.

86. The UTPCPL prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" 73 P.S. § 201-3.

87. This Count is brought for MGM's unfair and deceptive conduct, including MGM's unlawful and unfair and deceptive acts and practices, which "creat[ed] a likelihood of confusion or of misunderstanding" for Plaintiff and Class members as meant by 73 P.S. § 201-2(4)(xxi).

88. MGM engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the goods purchased by Plaintiff and the Class in violation of 73 P.S. § 201-3, including but not limited to the following:

a. MGM failed to enact adequate privacy and security measures to protect Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the July 2019 data breach;

b. MGM negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which ultimately was unfair and deceptive given the inadequacy of its privacy and security protections; and

c. MGM's negligence in failing to disclose the material fact of the inadequacy of its privacy and security protections for Plaintiff and Class members was unfair and deceptive.

89. The above unfair and deceptive acts and practices by MGM were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

90. MGM knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff's and Class members' PII and that risk of a data breach or theft was highly likely. MGM's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and reckless with respect to the rights of members of the Class.

91. Plaintiff and Class members relied on MGM's unfair and deceptive acts and

practices when they paid money in exchange for goods and services and provided their PII to MGM.

92. Plaintiff and Class members relied on MGM to safeguard and protect their PII and to timely and accurately notify them if their data had been breached and compromised.

93. Plaintiff and Class members seek all available relief under the UTPCPL, 73 P.S. § 201-1, *et seq.*

FIFTH CLAIM FOR RELIEF

(For Violation of Nevada's Consumer Fraud Act, Nevada Revised Statutes 41.600)

94. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

95. MGM engaged in unfair and unlawful acts and practices by failing to maintain adequate procedures to avoid a data breach, and permitting access to PII by data thieves, for whom MGM had no reasonable grounds to believe would be used for a proper purpose. Plaintiff and Class members relied on MGM's implied promise of data security when providing their PII to MGM.

96. MGM conduct violated NRS 598.0917(7) because it constituted a tender of "goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised," *i.e.*, goods offered for sale by credit card without the corresponding promise that a consumer's PII would be kept reasonably safe from harm.

97. MGM's violations of NRS 598.0917(7) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

98. MGM also breached its duty under NRS 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to

"implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." MGM did not take such reasonable security measures, as demonstrated by the unauthorized access of its network system.

99. MGM's violations of NRS 598.0923(3) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

100. Additionally, NRS 598.0923(3) provides that a violation of any federal or Nevada law constitutes consumer fraud. Thus, MGM violations of the FTC Act, NRS 598.0917(7), and NRS 603A violated NRS 598.0923(3).

101. MGM's violations of NRS 598.0923(3), NRS 598.0917(7), and NRS 603A in turn constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

102. MGM engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Class members.

103. As a direct and proximate result of the foregoing, Plaintiff and Class members have suffered injuries including, but not limited to, actual damages and in being denied a benefit conferred on them by the Nevada legislature.

104. As a result of these violations, Plaintiff and Class members are entitled to an award of actual damages, equitable injunctive relief, as well as an award of reasonable attorneys' fees and costs. Plaintiff and Class members also seek declaratory relief pursuant to 28 U.S.C. § 2201, specifically an order declaring that MGM' data security procedures violated applicable standards, which led to the exposure of the PII of Plaintiff and Class members in the data breach.

SIXTH CLAIM FOR RELIEF

(Unjust Enrichment)

105. Plaintiff repeats, realleges, and incorporates by reference the allegations

contained in each and every paragraph above, as though fully stated herein.

106. Plaintiff and Class members conferred a monetary benefit on MGM. Specifically, they purchased goods and services from MGM and in so doing provided MGM with their PII. In exchange, Plaintiff and Class members should have received from MGM the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

107. Defendant knew that Plaintiff and Class members conferred a benefit, which Defendant accepted. Defendant profited from these transactions but failed to protect the PII of Plaintiff and Class members.

108. The amounts Plaintiff and Class members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

109. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

110. Defendant failed to secure Plaintiff's and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

111. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

112. If Plaintiff and Class members knew that Defendant had not secured their PII, they would not have agreed to Defendant's services.

113. Plaintiff and Class members have no adequate remedy at law.

114. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class members.

115. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

116. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, Kevin V. Horne, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class members;

B. Designate Plaintiff as representative of the Class and the undersigned counsel as Class Counsel;

C. Award Plaintiff and the Class compensatory damages in an amount to be determined by the Court and treble and punitive damages to punish Defendant's egregious conduct as described herein, and to deter Defendant and others from engaging in similar conduct;

D. Award Plaintiff and the Class injunctive relief, as permitted by law or equity, including enjoining Defendant from continuing the unlawful practices set forth herein, ordering Defendant to fully disclose the extent and nature of the security breach and theft, and ordering Defendant to pay for not less than three years of identity theft and credit card monitoring services for Plaintiff and the Class;

E. Award Plaintiff and the Class statutory interest and penalties;

F. Award Plaintiff and the Class their costs, prejudgment and post judgment interest, and attorneys' fees; and

G. Grant such other relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all issues stated herein, and all issues so triable.

Dated: February 26, 2020

Respectfully submitted:

MUEHLBAUER LAW OFFICE, LTD.

By: /s/ Andrew R. Muehlbauer
ANDREW R. MUEHLBAUER, ESQ.
Nevada Bar No. 10161
7915 West Sahara Avenue, Suite 104
Las Vegas, Nevada 89117
Telephone: 702.330.4505
Facsimile: 702.825.0141
Email: andrew@mlolegal.com

LOWEY DANNENBERG, P.C.
Christian Levis (*pro hac* vice forthcoming)
Henry Kusjanovic (*pro hac* vice forthcoming)
Amanda Fiorilla (*pro hac* vice forthcoming)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
hkusjanovic@lowey.com
afiorilla@lowey.com

LOWEY DANNENBERG, P.C.
Anthony M. Christina (*pro hac* vice forthcoming)
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA
Telephone: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

Counsel for Plaintiff